Midterm Exam – MATH 311W Section 003
(Solutions Included)

Stephen G. Simpson
Pennsylvania State University

October 17, 2011

There are 6 problems on 6 pages. For each problem, use the space below the problem to exhibit your work leading to the solution of the problem. Give reasons for your answers. Please write neatly and do not show scratch work. For scratch work, you may use the back of each page. Whatever you write on the back of the page will not be graded.

1. (a) Use the Euclidean algorithm to find the greatest common divisor of 333 and 217.

   (b) Is 217 invertible modulo 333? Explain your answer.

   Solution.

   (a) The Euclidean algorithm consists of taking successive remainders. Applying the algorithm, we have
   $\mathrm{Rem}(333, 217) = 116$,
   $\mathrm{Rem}(217, 116) = 101$,
   $\mathrm{Rem}(116, 101) = 15$,
   $\mathrm{Rem}(101, 15) = 11$,
   $\mathrm{Rem}(15, 11) = 4$,
   $\mathrm{Rem}(11, 4) = 3$,
   $\mathrm{Rem}(4, 3) = 1$,
   $\mathrm{Rem}(3, 1) = 0$,
   so finally $\mathrm{GCD}(333, 217) = 1$.

   (b) One of our theorems states that, in general, a is invertible mod n if and only if a is relatively prime to n, or in other words, $\mathrm{GCD}(a, n) = 1$. In our present situation, $\mathrm{GCD}(217, 333) = 1$ so 217 is invertible mod 333.

2. Use the so-called "matrix method" to find integers x and y such that $333x + 217y =$ the greatest common divisor of 333 and 217.

   Solution. Instead of the matrix method as presented on pages 10–11 of the textbook, we use the matrix method as presented in class. Our matrix is such that each row $x\ y\ z$ of the matrix represents an equation $333x+217y = z$. The first row represents the equation $333\cdot 1+217\cdot 0 = 333$. The second row represents the equation $333 \cdot 0 + 217 \cdot 1 = 217$. Applying elementary row operations, we have

$$\begin{array}{rrr} 1 & 0 & 333 \\ 0 & 1 & 217 \\ 1 & -1 & 116 \\ -1 & 2 & 101 \\ 2 & -3 & 15 \\ -13 & 20 & 11 \\ 15 & -23 & 4 \\ -43 & 66 & 3 \\ 58 & -89 & 1 \end{array}$$

   and the last row represents the equation $333 \cdot 58 + 217 \cdot (-89) = 1$. Thus the solution of our problem is $x = 58$, $y = -89$.

3. Exhibit the unique factorization of 29304 into prime powers.

   Solution. We have $29304 = 8 \cdot 3663 = 8 \cdot 9 \cdot 407 = 8 \cdot 9 \cdot 11 \cdot 37$. Thus our factorization into prime powers is $29304 = 2^3 \cdot 3^2 \cdot 11 \cdot 37$.

4. (a) Find $\phi(29304)$. (Here ϕ is the Euler phi-function.)

   (b) What does Euler's Theorem tell us about arithmetic modulo 29304?

   Solution.

   (a) Using our factorization of 29304 into prime powers, we have
   $\phi(29304) = \phi(2^3)\phi(3^2)\phi(11)\phi(37)$
   $= (2^3 - 2^2)(3^2 - 3)(10)(36) = 4 \cdot 6 \cdot 10 \cdot 36 = 8640$.

   (b) In general, Euler's Theorem says that $a^{\phi(n)} \equiv 1 \bmod n$ whenever a is relatively prime to n. In our present situation, Euler's Theorem says that $a^{8640} \equiv 1 \bmod 29304$ for all a such that a is relatively prime to 29304.

5. For each of the following congruences, describe the solution set.

   (a) $56x \equiv 7 \bmod 134$.

   (b) $56x \equiv 111 \bmod 165$.

   (c) $56x \equiv 2 \bmod 91$.

   Solution. We rely on Theorem 1.5.1 in the textbook.

   (a) The prime factorizations of 56 and 134 are $56 = 2^3 \cdot 7$ and $134 = 2 \cdot 67$. Hence $\text{GCD}(56, 134) = 2$. Since 2 is not a divisor of 7, it follows that the congruence $56x \equiv 7 \bmod 134$ has no solutions.

   (b) The prime factorization of 165 is $165 = 3 \cdot 5 \cdot 11$. From this we see that $\text{GCD}(56, 165) = 1$. Since 1 is a divisor of 111, it follows that the congruence $56x \equiv 111 \bmod 165$ has exactly one solution mod 165. Calculations show that the inverse of 56 mod 165 is 56, and that $111 \cdot 56 \equiv 111 \bmod 165$. Thus the solution set of $56x \equiv 111 \bmod 165$ consists of all integers congruent to 111 mod 165.

   (c) The prime factorization of 91 is $91 = 7 \cdot 13$, hence $\text{GCD}(56, 91) = 7$. Since 7 is not a divisor of 2, it follows that the congruence $56x \equiv 2 \bmod 91$ has no solutions.

6. Prove that a is invertible modulo n if and only if $\text{GCD}(a, n) = 1$.

   Solution. Our proof will rely on the following known theorem:

   > For any integers a and b, the GCD of a and b is equal to the smallest positive integral linear combination of a and b.

   We now present our proof.

   First, assume that a is invertible mod n. This means that for some b we have $ab \equiv 1 \bmod n$. In other words, $ab - 1$ is divisible by n. Letting $k = \text{Quot}(ab - 1, n)$ we have $ab - 1 = kn$, or equivalently $ab - kn = 1$. Thus 1 is an integral linear combination of a and n. Therefore, our theorem noted above implies that $\text{GCD}(a, n) = 1$.

   Second, assume that $\text{GCD}(a, n) = 1$. By our theorem noted above, let r and s be integers such that $ra + sn = 1$. Then $ra - 1 = -sn$ is divisible by n, hence $ra \equiv 1 \bmod n$. In other words, r is an inverse of a modulo n. Thus a is invertible modulo n.

   This completes the proof.